(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(54) Title: TOKEN AUTHENTICATION SYSTEM AND METHOD
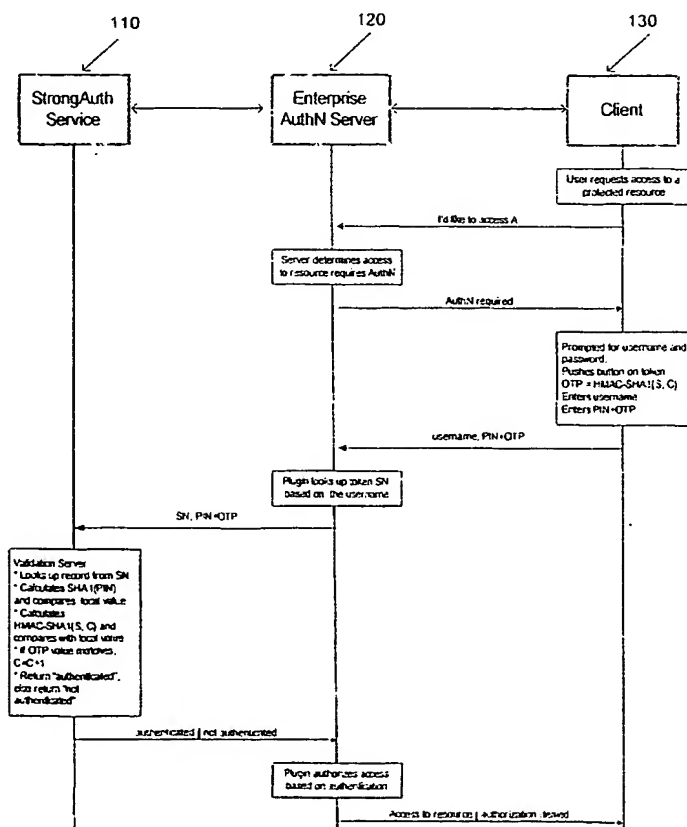
(57) Abstract: A method for calculating a One
Time Password. A secret is concatenated with a
count, where the secret is uniquely assigned to a
token. The secret can be a private key or a shared
secret symmetric key. The count is a number that
increases monotonically at the token with the number
of one-time Passwords generated at the token. The
count is also tracked at an authentication server, where
it increases monotonically with each calculation of
a one-time Password at the authentication server. An
OTP can be calculated by hashing a concatenated
secret and count. The result can be truncated.

WO 2005/083610 A1

FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE. AG. AL. AM. AT. AU. AZ. BA. BB. BG. BR. BW. BY. BZ. CA. CH. CN. CO. CR. CU. CZ. DE. DK. DM. DZ. EC. EE. EG. ES. FI. GB. GD. GE. GH. GM. HR. HU. ID. IL. IN. IS. JP. KE. KG. KP. KR. KZ. LC. LK. LR. LS. LT. LU. LV. MA. MD. MG. MK. MN. MW. MX. MZ. NA. NI. NO. NZ. OM. PG. PH. PL. PT. RO. RU. SC. SD. SE. SG. SK. SL. SM. SY. TJ. TM. TN. TR. TT. TZ. UA. UG. UZ. VC. VN. YU. ZA. ZM. ZW. ARIPO patent (BW. GH. GM. KE. LS. MW. MZ. NA. SD. SL. SZ. TZ. UG. ZM. ZW). Eurasian patent (AM. AZ. BY. KG. KZ. MD. RU. TJ. TM). European patent (AT. BE. BG. CH. CY. CZ. DE. DK. EE. ES. FI. FR. GB. GR. HU. IE. IS. IT. LT. LU. MC. NL. PL. PT. RO. SE. SI. SK. TR). OAPI patent (BF. BJ. CF. CG. CI. CM. GA. GN. GQ. GW. ML. MR. NE. SN. TD. TG)*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for the following designations AE. AG. AL. AM. AT. AU. AZ. BA. BB. BG. BR. BW.* BY. BZ. CA. CH. CN. CO. CR. CU. CZ. DE. DK. DM. DZ. EC. EE. EG. ES. FI. GB. GD. GE. GH. GM. HR. HU. ID. IL. IN. IS. JP. KE. KG. KP. KR. KZ. LC. LK. LR. LS. LT. LU. LV. MA. MD. MG. MK. MN. MW. MX. MZ. NA. NI. NO. NZ. OM. PG. PH. PL. PT. RO. RU. SC. SD. SE. SG. SK. SL. SM. SY. TJ. TM. TN. TR. TT. TZ. UA. UG. UZ. VC. VN. YU. ZA. ZM. ZW. ARIPO patent (BW. GH. GM. KE. LS. MW. MZ. NA. SD. SL. SZ. TZ. UG. ZM. ZW). Eurasian patent (AM. AZ. BY. KG. KZ. MD. RU. TJ. TM). European patent (AT. BE. BG. CH. CY. CZ. DE. DK. EE. ES. FI. FR. GB. GR. HU. IE. IS. IT. LT. LU. MC. NL. PL. PT. RO. SE. SI. SK. TR). OAPI patent (BF. BJ. CF. CG. CI. CM. GA. GN. GQ. GW. ML. MR. NE. SN. TD. TG)

Published:

— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.